In the Claims

1. (Currently Amended) A method of enforcing geographical restrictions on content redistribution in a TCP/IP network **in which content is distributed in packet form, each packet including header data and content data, the header data comprising information about the packet and its payload, the method comprising the acts** ~~, comprising~~:

defining a geographical boundary across which certain content **data** does not pass, wherein said boundary is defined – at least in part – by a hardware firewall device; and

determining whether an IP packet should be regarded as conveying content that should not cross said boundary, by reference to one or more **single-bit flags** ~~flag bits~~ included in the header **data** of said packet;

wherein said one or more flag bits are related to the payload of a watermark in the content **data**.

2-3. (Canceled)

4. (Currently Amended) A method of **providing entertainment content from a distributor to a home, while governing potential redistribution of the content from the home, the method including** ~~data processing that includes~~ forming an IP packet having header data and body data, wherein the **body data includes content data, and the** header data includes a first destination address **within the home to which the distributor intends the content data be delivered**, the method comprising:

the distributor forming said header data to additionally include additional data specifying whether it is permissible to send a copy of **the content** data in the packet to a second destination address **different than the first destination address**, wherein the additional data has at least two states, respectively indicating:

(a) it is not permissible to send a copy of **the content** data in the packet to any second destination address; or

(b) it is not permissible to send a copy of **the content** data in the packet to any

second destination address except to a second destination address within a domain that also includes the first destination address; and

wherein said domain comprises networked devices associated with a single family**, and restriction on potential redistribution of the content is defined by reference to the intended first address**.

5-6. (Canceled)

7. (Original) The method of claim 4 wherein a device associated with the first destination address has a first physical location and a device associated with the second destination address has a second physical location, and the additional data includes a field signaling that copying of data in said packet to said second destination address should be:

(a) permitted if the second physical location is physically proximate to the first physical location; and

(b) prohibited if the second physical location is physically remote from the first physical location.

8. (Original) The method of claim 7 wherein the first and second destination addresses are within a common domain.

9. (Original) The method of claim 7 wherein the first and second destination addresses both correspond to network devices associated with a single family.

10. (Original) The method of claim 4 wherein said additional data is related to the payload of a watermark encoded in the body data.

11. (Currently Amended) A method of data processing that includes receiving an IP packet having header data and body data, wherein the header data includes a first destination address, the first destination address corresponding to a device at a first physical location **where delivery of the packet was intended by an originator thereof, the body data comprising content data,** ~~**proximate to where said method is**~~

~~practiced,~~ the method comprising **– at said first physical location -** interpreting additional data in the header of said packet as specifying whether it is permissible to ~~send~~ **re-transmit** a copy of data in the packet **- after receipt thereof at the first destination address -** to a second destination address, wherein:

(a) if the additional data has a first state, prohibiting **re-**transmission of a copy of **the content** data in the packet to any second destination address; and

(b) if the additional data has a second state, prohibiting **re-**transmission of a copy of data in the packet to any second destination address other than a second destination address within a domain that also includes the first destination address.

12. (Canceled)

13. (Previously Presented) The method of claim 11, wherein said domain comprises networked devices associated with a single family.

14. (Original) The method of claim 11 wherein a device associated with the second destination address has a second physical location and wherein:

(a) if the second physical location is physically proximate to the first physical location, permitting copying of data in said packet to the second destination address; and

(b) if the second physical location is physically remote from the first physical location, prohibiting copying of data in said packet to the second destination address.

15. (Original) The method of claim 14 wherein the first and second destination addresses are within a common domain.

16. (Original) The method of claim 14 wherein the first and second destination addresses both correspond to network devices associated with a single family.

17. (Original) The method of claim 14 wherein the method includes determining whether the second physical location is physically remote from the first physically location by reference to whether the second destination address is served by a common

firewall with the first destination address.

18. (Original) The method of claim 11 wherein said additional data is related to the payload of a watermark encoded in the body data.

19-24. (Canceled)

25. (Previously Presented) A method of deterring unauthorized redistribution of video entertainment from a consumer's home network, the consumer's home network employing at least a computing device and a networking device;

wherein acts performed by the computing device include:

ascertaining restriction information for the video entertainment, said ascertaining including at least one of: (a) extracting restriction information from header data conveyed with the video entertainment; (b) obtaining restriction information from a remote repository associated with the video entertainment; or (c) discerning the restriction information by reference to data decoded from digital watermark information hidden within the video entertainment;

dividing the video entertainment among payload portions of plural IP packets;

including data indicating said ascertained restriction information in header portions of each of said IP packets; and

sending the packets to the networking device;

and wherein acts performed by the networking device comprise examining said included data and refusing to transmit the packets through the networking device to a different network if the included data indicates that the video entertainment should not be redistributed from the consumer's home network.

26. (Previously Presented) The method of claim 25 wherein the ascertaining includes extracting restriction information from header data conveyed with the video entertainment.

27. (Previously Presented) The method of claim 25 wherein the ascertaining includes obtaining restriction information from a remote repository associated with the video entertainment.

28. (Previously Presented) The method of claim 25 wherein the ascertaining includes discerning the restriction information by reference to data decoded from digital watermark information hidden within the video entertainment.

29. (New) The method of claim 1 wherein the determining comprises determining by reference to one single-bit flag.

30. (New) The method of claim 4 wherein the additional data comprises a single bit flag, indicating either the first or second state.

31. (New) The method of claim 11 wherein the additional data comprises a single bit flag, indicating either the first or second state.